

REPRESENTATION OF UNITS IN CYCLOTOMIC FUNCTION FIELDS

NGUYEN NGOC DONG QUAN

CONTENTS

1. Introduction	1
2. Some basic notions	3
2.1. The Galois group $\text{Gal}(\mathbb{K}_\varphi/\mathbf{k})$	3
2.2. Representation of integers in \mathcal{O}_φ , and the multiplicative group \mathcal{G}_φ	4
3. Representation of units	6
References	15

1. INTRODUCTION

Let q be a power of a prime p , and let \mathbb{F}_q denote the finite field with q elements. Let $\mathbf{A} = \mathbb{F}_q[T]$ be the ring of polynomials in the variable T over \mathbb{F}_q , and let $\mathbf{k} = \mathbb{F}_q(T)$ be the quotient field of \mathbf{A} . Let \mathbf{k}^{alg} denote an algebraic closure of \mathbf{k} . Let τ be the mapping defined by $\tau(x) = x^q$, and let $\mathbf{k}\langle\tau\rangle$ denote the twisted polynomial ring. Let $C : \mathbf{A} \rightarrow \mathbf{k}\langle\tau\rangle$ ($a \mapsto C_a$) be the Carlitz module, namely, C is an \mathbb{F}_q -algebra homomorphism such that $C_T = T + \tau$.

Let m be a polynomial of positive degree, and set $\Lambda_m = \{\lambda \in \mathbf{k}^{\text{alg}} \mid C_m(\lambda) = 0\}$. We define a *primitive m -th root of C* to be a root of the polynomial $C_m(x) \in \mathbf{A}[x]$ that generates the \mathbf{A} -module Λ_m . Throughout the paper, for each polynomial m , we fix a primitive m -th root of C , and denote it by λ_m . The *m -th cyclotomic function field*, denoted by \mathbb{K}_m , is defined by $\mathbb{K}_m = \mathbf{k}(\Lambda_m) = \mathbf{k}(\lambda_m)$. It is known (see Hayes [3], or Rosen [6]) that \mathbb{K}_m is a field extension of \mathbf{k} of degree $\Phi(m)$, where $\Phi(\cdot)$ is a function field analogue of the classical Euler ϕ -function. (We will recall the definition of $\Phi(\cdot)$ in Section 2.)

There are many strong analogies between the m -th cyclotomic function fields \mathbb{K}_m and the classical cyclotomic fields $\mathbb{Q}(\zeta_m)$ (see Goss [2], Hayes [3], Rosen [6], or Thakur [7]). Here the former letter m denotes a polynomial of positive degree in \mathbf{A} , and the latter letter m stands for a positive integer in \mathbb{Z} . In this paper, we are interested in studying new analogous phenomena between the cyclotomic function fields and the classical cyclotomic fields.

Newman [5] proved a refinement of Hilbert's Satz 90 for the extensions $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, where $p > 3$ is a prime, and ζ_p denotes the p -th root of unity. Recall that for a unit ϵ of norm 1 in $\mathbb{Z}[\zeta_p]$, Hilbert's Satz 90 (see Lang [4]) tells us that one can write ϵ as a quotient of conjugate integers in $\mathbb{Z}[\zeta_p]$, i.e., there exists an element $\delta \in \mathbb{Z}[\zeta_p]$ and an element $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ such that $\epsilon = \frac{\delta}{\sigma(\delta)}$. Newman (see [5, Corollary, p.357]) gave a refinement of Hilbert's Satz

90 by proving a sufficient and necessary condition for which such an element δ can be chosen to be a unit in $\mathbb{Z}[\zeta_p]$, and thus ϵ is a quotient of conjugate units in $\mathbb{Z}[\zeta_p]$. In order to obtain this result, Newman proved a stronger result that provides a unique representation of a unit

of norm 1 as a product of a power of a unit $\frac{1 - \zeta_p^e}{1 - \zeta_p}$ with a quotient of conjugate units. More precisely, Newman proved the following.

Theorem 1.1. (Newman, see [5, Theorem, p.353])

Let e be a primitive root modulo p , and let σ_e be a generator of the Galois group $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ that sends ζ_p to ζ_p^e . Let \mathcal{G}_p be the multiplicative group consisting of all units of the form $\frac{\delta}{\sigma_e(\delta)}$, where δ is a unit in $\mathbb{Z}[\zeta_p]$. Then for any unit ϵ of norm 1 in $\mathbb{Z}[\zeta_p]$, there exist an integer ℓ with $0 \leq \ell \leq p - 2$, and a unit $\alpha \in \mathcal{G}_p$ such that

$$\epsilon = \left(\frac{1 - \zeta_p^e}{1 - \zeta_p} \right)^\ell \alpha.$$

Furthermore the above representation is unique, i.e., if $\epsilon = \left(\frac{1 - \zeta_p^e}{1 - \zeta_p} \right)^{\ell_\star} \alpha_\star$ for some integer ℓ_\star with $0 \leq \ell_\star \leq p - 2$ and some unit $\alpha_\star \in \mathcal{G}_p$, then $\ell_\star = \ell$ and $\alpha_\star = \alpha$.

The aim of this paper is to prove a function field analogue of the above theorem, which can be viewed as a refinement of Hilbert's Satz 90 for the extensions $\mathbb{K}_\varphi/\mathbf{k}$. More explicitly, our main goal in this paper is to prove the following.

Theorem 1.2. (See Theorem 3.7 and Corollary 3.8)

Let φ be a monic prime in \mathbf{A} . Let \mathbb{K}_φ be the φ -th cyclotomic function field, and let \mathcal{O}_φ be the ring of integers of \mathbb{K}_φ . Let \mathfrak{g} be a primitive root modulo φ , and let $\sigma_\mathfrak{g}$ be a generator of the Galois group $\text{Gal}(\mathbb{K}_\varphi/\mathbf{k})$ that sends λ_φ to $C_\mathfrak{g}(\lambda_\varphi)$. Let \mathcal{G}_φ be the multiplicative group consisting of all units of the form $\frac{\delta}{\sigma_\mathfrak{g}(\delta)}$, where δ is a unit in \mathcal{O}_φ . Then for any unit ϵ of norm 1 in \mathcal{O}_φ , there exist an integer ℓ with $0 \leq \ell \leq q^{\deg(\varphi)} - 2$, and a unit $\alpha \in \mathcal{G}_\varphi$ such that

$$\epsilon = \left(\frac{\lambda_\varphi}{C_\mathfrak{g}(\lambda_\varphi)} \right)^\ell \alpha.$$

Furthermore the above representation is unique, i.e. if $\epsilon = \left(\frac{\lambda_\varphi}{C_\mathfrak{g}(\lambda_\varphi)} \right)^{\ell_\star} \alpha_\star$ for some integer ℓ_\star with $0 \leq \ell_\star \leq q^{\deg(\varphi)} - 2$ and some unit $\alpha_\star \in \mathcal{G}_\varphi$, then $\ell_\star = \ell$ and $\alpha_\star = \alpha$.

One can replace $\frac{1 - \zeta_p^e}{1 - \zeta_p}$ in Theorem 1.1 by its inverse $\frac{1 - \zeta_p}{1 - \zeta_p^e}$, and obtain a similar representation for units of norm 1 that is equivalent to that of Theorem 1.1. It is well-known (see Rosen [6, Proposition 12.6]) that $\frac{\lambda_\varphi}{C_\mathfrak{g}(\lambda_\varphi)}$ is a unit in \mathcal{O}_φ , and is a function field analogue of the unit $\frac{1 - \zeta_p}{1 - \zeta_p^e}$ in the number field setting. Hence Theorem 1.2 can be viewed as a function field analogue of Newman's theorem.

Using the same ideas as in Newman [5], we also obtain a sufficient and necessary condition for which a unit of norm 1 in \mathcal{O}_φ can be written as a quotient of conjugate units. This is a refinement of Hilbert's Satz 90 for the extensions $\mathbb{K}_\varphi/\mathbf{k}$.

The structure of the paper is as follows. In Section 2, we recall some basic notions and notation that will be used throughout the paper. In Section 3, we prove Theorem 1.2 (see Theorem 3.7 and Corollary 3.8), and consequently obtain a refinement of Hilbert's Satz 90 (see Corollary 3.10). The proof of Theorem 1.2 uses the same ideas and approach as in the proof of Newman [5, Theorem], but we need to introduce some modifications in many places to adapt Newman's proof of [5, Theorem] into the function field setting.

2. SOME BASIC NOTIONS

The aim of this section is to recall some basic notions and fix some notation that will be used throughout the paper.

For a polynomial $m \in \mathbf{A}$ of positive degree, we define $\Phi(m)$ to be the number of nonzero polynomials of degree less than $\deg(m)$ and relatively prime to m . The function $\Phi(\cdot)$ is a function field analogue of the classical Euler ϕ -function.

Let $m = \alpha \wp_1^{s_1} \cdots \wp_h^{s_h}$ be the prime factorization of m , where $\alpha \in \mathbb{F}_q^\times$, the \wp_i are monic primes in \mathbf{A} , and the s_i are positive integers. It is well-known (see [6, Proposition 1.7]) that

$$\Phi(m) = \prod_{i=1}^h \Phi(\wp_i^{s_i}) = \prod_{i=1}^h (q^{\deg(\wp_i^{s_i})} - q^{\deg(\wp_i^{s_i-1})}).$$

In particular, when $m = \wp^s$ for some monic prime \wp and some positive integer s ,

$$\Phi(\wp^s) = q^{\deg(\wp^s)} - q^{\deg(\wp^{s-1})}.$$

Recall that the m -th cyclotomic polynomial, denoted by $\Psi_m(x)$, is the minimal polynomial of λ_m over \mathbf{k} . It is well-known (see Hayes [3], or Rosen [6]) that $\Psi_m(x)$ is the monic irreducible polynomial of degree $\Phi(m)$ with coefficients in \mathbf{A} such that $\Psi_m(\lambda_m) = 0$.

When $m = \wp^s$ for some monic prime \wp and some positive integer s , we know from [3, Proposition 2.4] that

$$(1) \quad \Psi_{\wp^s}(x) = C_{\wp^s}(x) / C_{\wp^{s-1}}(x).$$

From Rosen [6, Proposition 12.11], one can write

$$C_{\wp}(x) = \wp x + [\wp, 1]x^q + \cdots + [\wp, \deg(\wp) - 1]x^{q^{\deg(\wp)-1}} + x^{q^{\deg(\wp)}},$$

where $[\wp, i] \in \mathbf{A}$ for each $1 \leq i \leq \deg(\wp) - 1$. For $s = 1$, the equation (1) tells us that

$$(2) \quad \Psi_{\wp}(x) = \frac{C_{\wp}(x)}{x} = \wp + [\wp, 1]x^{q-1} + \cdots + [\wp, \deg(\wp) - 1]x^{q^{\deg(\wp)-1}-1} + x^{q^{\deg(\wp)}-1}.$$

When $x = 0$, we obtain the following elementary result that will be useful in the proof of our main theorem.

Proposition 2.1. $\Psi_{\wp}(0) = \wp$.

2.1. The Galois group $\text{Gal}(\mathbb{K}_{\wp}/\mathbf{k})$. For the rest of this paper, fix a monic prime \wp of positive degree. Let \mathbb{K}_{\wp} be the \wp -th cyclotomic function field, and let \mathcal{O}_{\wp} be the ring of integers of \mathbb{K}_{\wp} . To rule out the trivialities, we further assume that

$$(\star) \quad q > 2 \text{ or } \deg(\wp) > 1.$$

We denote by $\text{Gal}(\mathbb{K}_{\wp}/\mathbf{k})$ the Galois group of $\mathbb{K}_{\wp}/\mathbf{k}$. There is an isomorphism between $\text{Gal}(\mathbb{K}_{\wp}/\mathbf{k})$ and the multiplicative group $(\mathbf{A}/\wp\mathbf{A})^\times$ (see Rosen [6, Chapter 12]). For each element $m \in (\mathbf{A}/\wp\mathbf{A})^\times$, there exists an isomorphism $\sigma_m \in \text{Gal}(\mathbb{K}_{\wp}/\mathbf{k})$ that is uniquely determined by the relation $\sigma_m(\lambda_{\wp}) = C_m(\lambda_{\wp})$. The correspondence $\sigma_m \mapsto m$ is an isomorphism from $\text{Gal}(\mathbb{K}_{\wp}/\mathbf{k})$ into the group $(\mathbf{A}/\wp\mathbf{A})^\times$.

Throughout the paper, fix an element $\mathbf{g} \in \mathbf{A}$ such that \mathbf{g} is a primitive root modulo \wp , i.e., \mathbf{g} is a generator of the group $(\mathbf{A}/\wp\mathbf{A})^\times$. Note that the order of $(\mathbf{A}/\wp\mathbf{A})^\times$ is $\Phi(\wp) = q^{\deg(\wp)} - 1$, and thus one can write $(\mathbf{A}/\wp\mathbf{A})^\times = \langle \mathbf{g} \rangle = \{\mathbf{g}^e \mid 0 \leq e \leq q^{\deg(\wp)} - 2\}$. We will prove that the isomorphism $\sigma_{\mathbf{g}} \in \text{Gal}(\mathbb{K}_{\wp}/\mathbf{k})$ is a generator of the cyclic group $\text{Gal}(\mathbb{K}_{\wp}/\mathbf{k})$, i.e., for each $0 \leq e \leq q^{\deg(\wp)} - 2$, $\sigma_{\mathbf{g}^e}(\lambda_{\wp}) = \sigma_{\mathbf{g}}^e(\lambda_{\wp})$. Indeed, take an arbitrary integer e with

$2 \leq e \leq q^{\deg(\wp)} - 2$. By induction, we see that

$$\begin{aligned} \sigma_{\mathfrak{g}^e}(\lambda_\wp) &= C_{\mathfrak{g}^e}(\lambda_\wp) = C_{\mathfrak{g}^{e-1}}(C_{\mathfrak{g}}(\lambda_\wp)) \\ &= C_{\mathfrak{g}^{e-1}}(\sigma_{\mathfrak{g}}(\lambda_\wp)) \\ &= \sigma_{\mathfrak{g}}(C_{\mathfrak{g}^{e-1}}(\lambda_\wp)) \\ &= \sigma_{\mathfrak{g}}(\sigma_{\mathfrak{g}^{e-1}}(\lambda_\wp)) \\ &= \sigma_{\mathfrak{g}}(\sigma_{\mathfrak{g}}^{e-1}(\lambda_\wp)) \\ &= \sigma_{\mathfrak{g}}^e(\lambda_\wp). \end{aligned}$$

We summarize the above discussion in the following.

Proposition 2.2. *The isomorphism $\sigma_{\mathfrak{g}} \in \text{Gal}(\mathbb{K}_\wp/\mathbf{k})$ is a generator for the cyclic group $\text{Gal}(\mathbb{K}_\wp/\mathbf{k})$. More precisely, $\sigma_{\mathfrak{g}^e}(\lambda_\wp) = \sigma_{\mathfrak{g}}^e(\lambda_\wp)$ for each $0 \leq e \leq q^{\deg(\wp)} - 2$.*

Throughout the paper, we denote by $\text{Norm}_{\mathbb{K}_\wp/\mathbf{k}}(\cdot)$ the norm from \mathbb{K}_\wp to \mathbf{k} . Proposition 2.2 implies that for each element $\alpha \in \mathbb{K}_\wp^\times$,

$$\text{Norm}_{\mathbb{K}_\wp/\mathbf{k}}(\alpha) = \prod_{\sigma \in \text{Gal}(\mathbb{K}_\wp/\mathbf{k})} \sigma(\alpha) = \prod_{e=0}^{q^{\deg(\wp)}-2} \sigma_{\mathfrak{g}}^e(\alpha).$$

The following elementary result will be useful in the proof of our main theorem.

Proposition 2.3. *Let α be a unit in \mathcal{O}_\wp of norm 1. Then there exists an element $\delta \in \mathcal{O}_\wp$ such that*

$$\alpha = \frac{\delta}{\sigma_{\mathfrak{g}}(\delta)}.$$

Proof. Applying Hilbert's Satz 90 (see Lang [4]), there exists an element $\gamma \in \mathbb{K}_\wp$ such that

$$(3) \quad \alpha = \frac{\gamma}{\sigma_{\mathfrak{g}}(\gamma)}.$$

Since $\mathbb{K}_\wp = \mathbf{k}(\lambda_\wp)$, one can write

$$\gamma = \frac{\sum_i a_i \lambda_\wp^i}{b},$$

where the a_i are in \mathbf{A} , and $b \in \mathbf{A}^\times$. From (3), one gets

$$\alpha = \frac{\frac{\sum_i a_i \lambda_\wp^i}{b}}{\sigma_{\mathfrak{g}}\left(\frac{\sum_i a_i \lambda_\wp^i}{b}\right)} = \frac{\delta}{\sigma_{\mathfrak{g}}(\delta)},$$

where $\delta = \sum_i a_i \lambda_\wp^i \in \mathbf{A}[\lambda_\wp]$. Since $\mathcal{O}_\wp = \mathbf{A}[\lambda_\wp]$ (see Rosen [6, Proposition 12.9]), our contention follows. \square

2.2. Representation of integers in \mathcal{O}_\wp , and the multiplicative group \mathcal{G}_\wp . It is well-known (see [6, Proposition 12.9]) that $\mathcal{O}_\wp = \mathbf{A}[\lambda_\wp]$. For each polynomial $\mathcal{P}(x) \in \mathbf{A}[x]$ of degree $\leq q^{\deg(\wp)} - 2$, $\mathcal{P}(\lambda_\wp)$ is an integer in \mathcal{O}_\wp . Conversely we will prove that for each integer $\alpha \in \mathcal{O}_\wp$, there exists a unique polynomial $\mathcal{P}_\alpha(x) \in \mathbf{A}[x]$ of degree $\leq q^{\deg(\wp)} - 2$ such

that $\alpha = \mathcal{P}_\alpha(\lambda_\wp)$. Indeed we know that the minimal polynomial of λ_\wp is the \wp -th cyclotomic polynomial $\Psi_\wp(x) \in \mathbf{A}[x]$. From (1), $\Psi_\wp(x)$ can be explicitly written in the form

$$\Psi_\wp(x) = \frac{C_\wp(x)}{x},$$

and thus $\deg(\Psi_\wp(x)) = q^{\deg \wp} - 1$. Hence $\{\lambda_\wp^e\}_{0 \leq e \leq q^{\deg(\wp)} - 2}$ is a basis for the \mathbf{A} -module $\mathbf{A}[\lambda_\wp]$. Hence for each integer $\alpha \in \mathcal{O}_\wp$, there exists a polynomial $\mathcal{P}_\alpha(x) \in \mathbf{A}[x]$ of degree $\leq q^{\deg(\wp)} - 2$ such that $\alpha = \mathcal{P}_\alpha(\lambda_\wp)$. We prove that \mathcal{P}_α is unique. Assume the contrary, i.e., there exists a polynomial $\mathcal{Q}_\alpha(x) \in \mathbf{A}[x]$ of degree $\leq q^{\deg(\wp)} - 2$ such that $\mathcal{Q}_\alpha(x) \neq \mathcal{P}_\alpha(x)$, and $\alpha = \mathcal{Q}_\alpha(\lambda_\wp)$. Setting $F(x) = \mathcal{P}_\alpha(x) - \mathcal{Q}_\alpha(x) \in \mathbf{A}[x]$, we deduce that

$$F(\lambda_\wp) = \mathcal{P}_\alpha(\lambda_\wp) - \mathcal{Q}_\alpha(\lambda_\wp) = 0.$$

Since $\mathcal{Q}_\alpha(x) \neq \mathcal{P}_\alpha(x)$, the polynomial $F(x)$ is nonzero. Furthermore $F(x)$ is of degree at most $q^{\deg(\wp)} - 2$, which is a contradiction since $\Psi_\wp(x)$ is the minimal polynomial of λ_\wp and $\deg(\Psi_\wp(x)) = q^{\deg \wp} - 1 > q^{\deg(\wp)} - 2$.

We summarize the above discussion in the following.

Proposition 2.4. *For each integer $\alpha \in \mathcal{O}_\wp$, there exists a unique polynomial $\mathcal{P}_\alpha(x) \in \mathbf{A}[x]$ of degree at most $q^{\deg(\wp)} - 2$ such that $\alpha = \mathcal{P}_\alpha(\lambda_\wp)$. Furthermore $\alpha = 0$ if and only if the polynomial $\mathcal{P}_\alpha(x)$ is identical to zero.*

For the rest of the paper, for each integer $\alpha \in \mathcal{O}_\wp$, we always denote by \mathcal{P}_α the unique polynomial satisfying $\alpha = \mathcal{P}_\alpha(\lambda_\wp)$ in Proposition 2.4. We call \mathcal{P}_α the *polynomial representing* α .

Proposition 2.5. *Let α be a nonzero element in \mathcal{O}_\wp , and let $\mathcal{P}_\alpha(x) \in \mathbf{A}[x]$ be the polynomial representing α . If $\mathcal{Q}(x)$ is a polynomial in $\mathbf{A}[x]$ such that $\mathcal{Q}(\lambda_\wp) = \alpha$, then*

$$\frac{\mathcal{Q}(\lambda_\wp)}{\mathcal{Q}(C_\mathfrak{g}(\lambda_\wp))} = \frac{\mathcal{P}_\alpha(\lambda_\wp)}{\mathcal{P}_\alpha(C_\mathfrak{g}(\lambda_\wp))} = \frac{\alpha}{\sigma_\mathfrak{g}(\alpha)}.$$

Remark 2.6. Since $\alpha = \mathcal{Q}(\lambda_\wp) \neq 0$, and

$$\mathcal{Q}(C_\mathfrak{g}(\lambda_\wp)) = \mathcal{Q}(\sigma_\mathfrak{g}(\lambda_\wp)) = \sigma_\mathfrak{g}(\mathcal{Q}(\lambda_\wp)),$$

$\mathcal{Q}(C_\mathfrak{g}(\lambda_\wp))$ is also nonzero. Similarly $\mathcal{P}(C_\mathfrak{g}(\lambda_\wp))$ is nonzero.

Proof. From the assumption and Remark 2.6, we know that

$$\frac{\mathcal{Q}(\lambda_\wp)}{\mathcal{Q}(C_\mathfrak{g}(\lambda_\wp))} = \frac{\alpha}{\sigma_\mathfrak{g}(\alpha)}.$$

Similarly one also gets

$$\frac{\mathcal{P}_\alpha(\lambda_\wp)}{\mathcal{P}_\alpha(C_\mathfrak{g}(\lambda_\wp))} = \frac{\alpha}{\sigma_\mathfrak{g}(\alpha)},$$

and thus Proposition 2.5 follows. □

We now introduce the multiplicative group \mathcal{G}_\wp that will be of interest in this paper. Let \mathcal{G}_\wp be the set consisting of all elements of the form $\frac{\mathcal{Q}(\lambda_\wp)}{\mathcal{Q}(C_\mathfrak{g}(\lambda_\wp))}$, where $\mathcal{Q}(x) \in \mathbf{A}[x]$ such that $\mathcal{Q}(\lambda_\wp)$ is a unit in \mathcal{O}_\wp . From Proposition 2.5, we see that all the elements of \mathcal{G}_\wp are units in \mathcal{O}_\wp . Furthermore the set \mathcal{G}_\wp is invariant under the multiplication, i.e., $\epsilon\gamma \in \mathcal{G}_\wp$ for any $\epsilon, \gamma \in \mathcal{G}_\wp$. For an arbitrary element $\frac{\mathcal{Q}(\lambda_\wp)}{\mathcal{Q}(C_\mathfrak{g}(\lambda_\wp))} \in \mathcal{G}_\wp$, where $\mathcal{Q}(x) \in \mathbf{A}[x]$ such that $\alpha = \mathcal{Q}(\lambda_\wp)$ is a unit in \mathcal{O}_\wp . Note that α^{-1} is a unit in \mathcal{O}_\wp . Let $\mathcal{P}_{\alpha^{-1}}(x) \in \mathbf{A}[x]$ be the polynomial representing

α^{-1} . From Proposition 2.5, $\frac{\mathcal{P}_{\alpha^{-1}}(\lambda_\varphi)}{\mathcal{P}_{\alpha^{-1}}(C_{\mathfrak{g}}(\lambda_\varphi))} = \frac{\alpha^{-1}}{\sigma_{\mathfrak{g}}(\alpha^{-1})}$, and thus $\frac{\alpha^{-1}}{\sigma_{\mathfrak{g}}(\alpha^{-1})}$ belongs to \mathcal{G}_φ . By Proposition 2.5, we deduce that

$$\frac{\mathcal{Q}(\lambda_\varphi)}{\mathcal{Q}(C_{\mathfrak{g}}(\lambda_\varphi))} \frac{\alpha^{-1}}{\sigma_{\mathfrak{g}}(\alpha^{-1})} = \frac{\alpha}{\sigma_{\mathfrak{g}}(\alpha)} \frac{\alpha^{-1}}{\sigma_{\mathfrak{g}}(\alpha^{-1})} = 1,$$

which proves that $\frac{\alpha^{-1}}{\sigma_{\mathfrak{g}}(\alpha^{-1})}$ is the inverse of $\frac{\mathcal{Q}(\lambda_\varphi)}{\mathcal{Q}(C_{\mathfrak{g}}(\lambda_\varphi))}$. Hence \mathcal{G}_φ is a multiplicative group.

Throughout this paper, we denote by $\mathcal{U}_*(\mathcal{O}_\varphi)$ be the group of units of norm 1 in \mathcal{O}_φ . The following result follows immediately from the above discussion and Proposition 2.5.

Proposition 2.7.

- (i) \mathcal{G}_φ is a subgroup of $\mathcal{U}_*(\mathcal{O}_\varphi)$.
- (ii)

$$\mathcal{G}_\varphi = \left\{ \frac{\alpha}{\sigma_{\mathfrak{g}}(\alpha)} \mid \alpha \text{ is a unit in } \mathcal{O}_\varphi \right\}.$$

(iii)

$$\mathcal{G}_\varphi = \left\{ \frac{\mathcal{P}_\alpha(\lambda_\varphi)}{\mathcal{P}_\alpha(C_{\mathfrak{g}}(\lambda_\varphi))} \mid \alpha \text{ is a unit in } \mathcal{O}_\varphi, \text{ and } \mathcal{P}_\alpha(x) \in \mathbf{A}[x] \text{ is the polynomial representing } \alpha \right\}.$$

3. REPRESENTATION OF UNITS

In this section, we will prove Theorem 1.2 (see Theorem 3.7 and Corollary 3.8). As a consequence, we obtain a refinement of Hilbert's Satz 90 (see Corollary 3.10). We begin by proving several lemmas that we will need in the proof of our main theorem.

The next result is a function field analogue of Newman [5, Lemma 1]. We follow the same ideas as in the proof of Newman [5, Lemma 1] to prove the next lemma.

Lemma 3.1. *Let α be an integer in \mathcal{O}_φ , and let $\mathcal{P}_\alpha(x) \in \mathbf{A}[x]$ be the polynomial representing α . Assume that the following are true.*

- (i) $\frac{\mathcal{P}_\alpha(C_{\mathfrak{g}}(\lambda_\varphi))}{\mathcal{P}_\alpha(\lambda_\varphi)}$ is a unit in \mathcal{O}_φ . (Recall that \mathfrak{g} is a generator of the group $(\mathbf{A}/\varphi\mathbf{A})^\times$.)
- (ii) $\gcd(\mathcal{P}_\alpha(0), \varphi) = 1$.
- (iii) the content of the polynomial $\mathcal{P}_\alpha(x)$ is 1, i.e., the greatest common divisor of all coefficients of $\mathcal{P}_\alpha(x)$ is 1.

Then α is a unit in \mathcal{O}_φ .

Remark 3.2. By (ii) in Lemma 3.1, one sees that the polynomial $\mathcal{P}_\alpha(x)$ is nonzero, and it thus follows from Proposition 2.4 that $\alpha = \mathcal{P}_\alpha(\lambda_\varphi) \neq 0$.

Proof. Assume the contrary, i.e., α is a non-unit in \mathcal{O}_φ . Since $\alpha = \mathcal{P}_\alpha(\lambda_\varphi)$, $\mathcal{P}_\alpha(\lambda_\varphi)$ is also a non-unit in \mathcal{O}_φ . Hence there exists a prime ideal \mathfrak{q} in \mathcal{O}_φ that divides $\mathcal{P}_\alpha(\lambda_\varphi)$. Thus the ideal $\sigma_{\mathfrak{g}}(\mathfrak{q})$ is prime, and is a prime ideal divisor of $\sigma_{\mathfrak{g}}(\mathcal{P}_\alpha(\lambda_\varphi))$. Since

$$\sigma_{\mathfrak{g}}(\mathcal{P}_\alpha(\lambda_\varphi)) = \mathcal{P}_\alpha(\sigma_{\mathfrak{g}}(\lambda_\varphi)) = \mathcal{P}_\alpha(C_{\mathfrak{g}}(\lambda_\varphi)),$$

it follows that $\sigma_{\mathfrak{g}}(\mathfrak{q})$ is a prime ideal divisor of $\mathcal{P}_\alpha(C_{\mathfrak{g}}(\lambda_\varphi))$. We deduce from (i) that $\sigma_{\mathfrak{g}}(\mathfrak{q})$ is also a prime ideal divisor of $\mathcal{P}_\alpha(\lambda_\varphi)$. Since $\sigma_{\mathfrak{g}}$ is a generator of the Galois group $\text{Gal}(\mathbb{K}_\varphi/\mathbf{k})$, every conjugate of the prime ideal \mathfrak{q} is a prime ideal divisor of $\mathcal{P}_\alpha(\lambda_\varphi)$, i.e., for every element $\sigma \in \text{Gal}(\mathbb{K}_\varphi/\mathbf{k})$, $\sigma(\mathfrak{q})$ is a prime ideal divisor of $\mathcal{P}_\alpha(\lambda_\varphi)$.

We contend that $\gcd(\mathcal{P}_\alpha(\lambda_\varphi), \lambda_\varphi) = 1$; otherwise since $\lambda_\varphi \mathcal{O}_\varphi$ is a prime ideal in \mathcal{O}_φ (see Rosen [6, Proposition 12.7]), we deduce that $\lambda_\varphi \mathcal{O}_\varphi$ divides $\mathcal{P}_\alpha(\lambda_\varphi)$, and thus

$$\mathcal{P}_\alpha(0) \equiv \mathcal{P}_\alpha(\lambda_\varphi) \equiv 0 \pmod{\lambda_\varphi}.$$

Since $\wp \mathcal{O}_\wp = (\lambda_\wp \mathcal{O}_\wp)^{q^{\deg(\wp)}-1}$ (see Rosen [6, Proposition 12.7]), we deduce that $\mathcal{P}_\alpha(0) \equiv 0 \pmod{\wp}$, which is a contradiction to (ii).

Since the prime ideal $\sigma(\mathfrak{q})$ divides $\mathcal{P}_\alpha(\lambda_\wp)$ for every $\sigma \in \text{Gal}(\mathbb{K}_\wp/\mathbf{k})$, we deduce that $\sigma(\mathfrak{q}) \neq \lambda_\wp \mathcal{O}_\wp$ for every $\sigma \in \text{Gal}(\mathbb{K}_\wp/\mathbf{k})$. Since \mathfrak{q} is a prime ideal, we know that $\text{Norm}_{\mathbb{K}_\wp/\mathbf{k}}(\mathfrak{q}) = (\mathfrak{p}\mathbf{A})^r$ for some monic prime $\mathfrak{p} \in \mathbf{A}$ and some positive integer r . By [1, Theorem 3.5.1], and since $\wp \mathcal{O}_\wp = (\lambda_\wp \mathcal{O}_\wp)^{q^{\deg(\wp)}-1}$, we deduce that $\mathfrak{p} \neq \wp$. By Rosen [6, Proposition 12.7], \mathbb{K}_\wp is unramified at \mathfrak{p} , and thus $\mathfrak{p}\mathcal{O}_\wp$ is the product of the distinct conjugates of \mathfrak{q} . Therefore $\mathfrak{p}\mathcal{O}_\wp$ divides $\mathcal{P}_\alpha(\lambda_\wp)\mathcal{O}_\wp$, and thus

$$(4) \quad \frac{\mathcal{P}_\alpha(\lambda_\wp)}{\mathfrak{p}} \in \mathcal{O}_\wp.$$

By Remark 3.2, and since $\deg(\mathcal{P}_\alpha(x)) \leq q^{\deg(\wp)} - 2$, one can write

$$(5) \quad \mathcal{P}_\alpha(x) = \sum_{i=0}^h \epsilon_i x^i,$$

where the ϵ_i are in \mathbf{A} with $\epsilon_h \neq 0$, and $h = \deg(\mathcal{P}_\alpha(x)) \leq q^{\deg(\wp)} - 2$. By [6, Proposition 12.9], $\mathcal{O}_\wp = \mathbf{A}[\lambda_\wp]$, and since the minimal polynomial of λ_\wp over \mathbf{k} is the \wp -th cyclotomic polynomial $\Psi_\wp(x) \in \mathbf{A}[x]$ of degree exactly $q^{\deg(\wp)} - 1$ (see Hayes [3] or Section 2), it follows from (4) and (5) that there exists an element of the form $\sum_{j=0}^{q^{\deg(\wp)}-2} \kappa_j \lambda_\wp^j \in \mathcal{O}_\wp = \mathbf{A}[\lambda_\wp]$ with the $\kappa_j \in \mathbf{A}$ such that

$$\frac{\mathcal{P}_\alpha(\lambda_\wp)}{\mathfrak{p}} = \sum_{i=0}^h \frac{\epsilon_i}{\mathfrak{p}} \lambda_\wp^i = \sum_{j=0}^{q^{\deg(\wp)}-2} \kappa_j \lambda_\wp^j.$$

Therefore

$$(6) \quad \sum_{i=0}^h \left(\frac{\epsilon_i}{\mathfrak{p}} - \kappa_i \right) \lambda_\wp^i - \sum_{i=h+1}^{q^{\deg(\wp)}-2} \kappa_i \lambda_\wp^i = 0.$$

Since $h \leq q^{\deg(\wp)} - 2$ and the minimal polynomial of λ_\wp over \mathbf{k} is the \wp -th cyclotomic polynomial $\Psi_\wp(x) \in \mathbf{A}[x]$ of degree exactly $q^{\deg(\wp)} - 1$, we deduce from (6) that

$$\frac{\epsilon_i}{\mathfrak{p}} - \kappa_i = 0$$

for every $0 \leq i \leq h$. Thus $\epsilon_i = \mathfrak{p}\kappa_i$ for every $0 \leq i \leq h$. Therefore \mathfrak{p} divides $\gcd_{0 \leq i \leq h}(\epsilon_i)$. This implies that the content of $\mathcal{P}_\alpha(x)$ is divisible by \mathfrak{p} , which is a contradiction to (iii) in Lemma 3.1. Thus α is a unit in \mathcal{O}_\wp . \square

For each $e \geq 1$, set

$$(7) \quad \rho_e = \frac{\sigma_{\mathfrak{g}}^{e-1}(\lambda_\wp)}{\sigma_{\mathfrak{g}}^e(\lambda_\wp)} = \sigma_{\mathfrak{g}}^{e-1} \left(\frac{\lambda_\wp}{\sigma_{\mathfrak{g}}(\lambda_\wp)} \right).$$

Since $\frac{\lambda_\wp}{\sigma_{\mathfrak{g}}(\lambda_\wp)} = \frac{\lambda_\wp}{C_{\mathfrak{g}}(\lambda_\wp)}$ is a unit in \mathcal{O}_\wp (see Rosen [6, Proposition 12.6]), it follows that ρ_e is a unit in \mathcal{O}_\wp . Recall from Subsection 2.1 that $\sigma_{\mathfrak{g}}^r(\lambda_\wp) = \sigma_{\mathfrak{g}^r}(\lambda_\wp) = C_{\mathfrak{g}^r}(\lambda_\wp)$; hence one can write (7) in the form

$$(8) \quad \rho_e = \frac{C_{\mathfrak{g}^{e-1}}(\lambda_\wp)}{C_{\mathfrak{g}^e}(\lambda_\wp)}.$$

Let $\mathcal{P}_{\rho_e}(x) \in \mathbf{A}[x]$ be the polynomial representing ρ_e . From the above equation, one gets

$$\mathcal{P}_{\rho_e}(C_{\mathfrak{g}}(\lambda_{\wp})) = \mathcal{P}_{\rho_e}(\sigma_{\mathfrak{g}}(\lambda_{\wp})) = \sigma_{\mathfrak{g}}(\mathcal{P}_{\rho_e}(\lambda_{\wp})) = \sigma_{\mathfrak{g}}(\rho_e) = \sigma_{\mathfrak{g}}\left(\frac{\sigma_{\mathfrak{g}}^{e-1}(\lambda_{\wp})}{\sigma_{\mathfrak{g}}^e(\lambda_{\wp})}\right),$$

and thus

$$(9) \quad \mathcal{P}_{\rho_e}(C_{\mathfrak{g}}(\lambda_{\wp})) = \frac{\sigma_{\mathfrak{g}}^e(\lambda_{\wp})}{\sigma_{\mathfrak{g}}^{e+1}(\lambda_{\wp})} = \rho_{e+1} = \mathcal{P}_{\rho_{e+1}}(\lambda_{\wp}).$$

Lemma 3.3. *Let ℓ be an integer ≥ 2 , and set*

$$\Lambda_{\wp} = \prod_{h=2}^{\ell} \prod_{e=2}^h \frac{\rho_e}{\rho_{e-1}} = \prod_{h=2}^{\ell} \prod_{e=2}^h \frac{\mathcal{P}_{\rho_{e-1}}(C_{\mathfrak{g}}(\lambda_{\wp}))}{\mathcal{P}_{\rho_{e-1}}(\lambda_{\wp})}.$$

Then

$$(10) \quad \frac{\lambda_{\wp}}{C_{\mathfrak{g}^{\ell}}(\lambda_{\wp})} = \Lambda_{\wp} \left(\frac{\lambda_{\wp}}{C_{\mathfrak{g}}(\lambda_{\wp})} \right)^{\ell}.$$

Proof. For each $h \geq 1$, we see that

$$\prod_{e=2}^h \frac{\rho_e}{\rho_{e-1}} = \frac{\rho_h}{\rho_1},$$

and it thus follows from (8) that

$$\Lambda_{\wp} = \prod_{h=2}^{\ell} \frac{\rho_h}{\rho_1} = \frac{1}{\rho_1^{\ell-1}} \prod_{h=2}^{\ell} \frac{C_{\mathfrak{g}^{h-1}}(\lambda_{\wp})}{C_{\mathfrak{g}^h}(\lambda_{\wp})} = \left(\frac{C_{\mathfrak{g}}(\lambda_{\wp})}{\lambda_{\wp}} \right)^{\ell-1} \frac{C_{\mathfrak{g}}(\lambda_{\wp})}{C_{\mathfrak{g}^{\ell}}(\lambda_{\wp})}.$$

Therefore (10) follows immediately. □

Let $\ell = q^{\deg(\wp)} - 1$. Note that (\star) in Subsection 2.1 implies that $\ell \geq 2$. Since

$$C_{\mathfrak{g}^{q^{\deg(\wp)}-1}}(\lambda_{\wp}) = \sigma_{\mathfrak{g}^{q^{\deg(\wp)}-1}}(\lambda_{\wp}) = \sigma_{\mathfrak{g}}^{q^{\deg(\wp)}-1}(\lambda_{\wp}) = \lambda_{\wp},$$

we deduce from Lemma 3.3 that

$$(11) \quad \Lambda_{\wp} = \left(\frac{\lambda_{\wp}}{C_{\mathfrak{g}}(\lambda_{\wp})} \right)^{1-q^{\deg(\wp)}}.$$

We summarize the above discussion in the following result.

Corollary 3.4. *Let ℓ be an integer. Then there exist an integer e with $0 \leq e \leq q^{\deg(\wp)} - 2$ and an integer h such that the following are true:*

- (i) $\ell = (q^{\deg(\wp)} - 1)h + e$; and
- (ii)

$$\left(\frac{\lambda_{\wp}}{C_{\mathfrak{g}}(\lambda_{\wp})} \right)^{\ell} = \left(\frac{\lambda_{\wp}}{C_{\mathfrak{g}}(\lambda_{\wp})} \right)^e \Lambda_{\wp}^{-h}.$$

From the definition of Λ_{\wp} in Lemma 3.3, Λ_{\wp}^{-1} clearly belongs to the multiplicative group \mathcal{G}_{\wp} , and so does Λ_{\wp}^h for any integer h . (Recall that \mathcal{G}_{\wp} is defined in Subsection 2.2.) From Proposition 2.7 and Corollary 3.4, we obtain the following result.

Corollary 3.5. *Let ℓ be an integer. Then there exist an integer e with $0 \leq e \leq q^{\deg(\wp)} - 2$ and an element $\frac{\mathcal{Q}(\lambda_\wp)}{\mathcal{Q}(C_{\mathfrak{g}}(\lambda_\wp))} \in \mathcal{G}_\wp$ such that*

$$\left(\frac{\lambda_\wp}{C_{\mathfrak{g}}(\lambda_\wp)} \right)^\ell = \left(\frac{\lambda_\wp}{C_{\mathfrak{g}}(\lambda_\wp)} \right)^e \frac{\mathcal{Q}(\lambda_\wp)}{\mathcal{Q}(C_{\mathfrak{g}}(\lambda_\wp))}.$$

Lemma 3.6. *Let $\mathcal{Q}(x)$ be a polynomial in $\mathbf{A}[x]$ such that $\mathcal{Q}(\lambda_\wp)$ is a unit in \mathcal{O}_\wp . Then $\gcd(\mathcal{Q}(0), \wp) = 1$.*

Proof. Let $\epsilon = \mathcal{Q}(\lambda_\wp)$. By assumption, ϵ is a unit in \mathcal{O}_\wp . Assume the contrary, i.e., \wp divides $\mathcal{Q}(0)$. It is known (see Rosen [6, Proposition 12.7]) that $\wp \mathcal{O}_\wp = (\lambda_\wp \mathcal{O}_\wp)^{q^{\deg(\wp)} - 1}$. Thus λ_\wp divides $\mathcal{Q}(0)$, and hence

$$\epsilon = \mathcal{Q}(\lambda_\wp) \equiv \mathcal{Q}(0) \equiv 0 \pmod{\lambda_\wp},$$

which is a contradiction since ϵ is a unit in \mathcal{O}_\wp and $\lambda_\wp \mathcal{O}_\wp$ is a prime ideal in \mathcal{O}_\wp (see Rosen [6, Proposition 12.7]). \square

The next result is our main theorem in this paper, which can be viewed as a function field analogue of Newman [5, Theorem]. The proof of the next theorem follows the same ideas as in the proof of Newman [5, Theorem], but we need some modifications to adapt the proof of Newman [5, Theorem] into the function field setting.

Theorem 3.7. *Let ϵ be a unit in \mathcal{O}_\wp of norm 1. Then there exist an integer ℓ with $0 \leq \ell \leq q^{\deg(\wp)} - 2$, and a polynomial $\mathcal{Q}(x) \in \mathbf{A}[x]$ of degree at most $q^{\deg(\wp)} - 2$ with $\mathcal{Q}(\lambda_\wp)$ being a unit in \mathcal{O}_\wp such that the following are true:*

(R1) ϵ can be represented in the form

$$\epsilon = \left(\frac{\lambda_\wp}{C_{\mathfrak{g}}(\lambda_\wp)} \right)^\ell \left(\frac{\mathcal{Q}(\lambda_\wp)}{\mathcal{Q}(C_{\mathfrak{g}}(\lambda_\wp))} \right).$$

(R2) *The representation of ϵ in (R1) is unique, except that $\mathcal{Q}(x)$ can be replaced by $v\mathcal{Q}(x)$ for some unit $v \in \mathbb{F}_q^\times$; more precisely, if there exist an integer ℓ_\star with $0 \leq \ell_\star \leq q^{\deg(\wp)} - 2$, and a polynomial $\mathcal{Q}_\star(x) \in \mathbf{A}[x]$ of degree at most $q^{\deg(\wp)} - 2$ with $\mathcal{Q}_\star(\lambda_\wp)$ being a unit in \mathcal{O}_\wp such that*

$$\epsilon = \left(\frac{\lambda_\wp}{C_{\mathfrak{g}}(\lambda_\wp)} \right)^{\ell_\star} \left(\frac{\mathcal{Q}_\star(\lambda_\wp)}{\mathcal{Q}_\star(C_{\mathfrak{g}}(\lambda_\wp))} \right),$$

then $\ell_\star = \ell$ and $\mathcal{Q}_\star(x) = v\mathcal{Q}(x)$ for some unit $v \in \mathbb{F}_q^\times$.

Proof. Let $\mathcal{P}_\epsilon(x) \in \mathbf{A}[x]$ be the polynomial representing ϵ , i.e., $\epsilon = \mathcal{P}_\epsilon(\lambda_\wp)$. By Lemma 3.6,

$$(12) \quad \gcd(\mathcal{P}_\epsilon(0), \wp) = 1.$$

By (12) and since \mathfrak{g} is a generator of the cyclic group $(\mathbf{A}/\wp\mathbf{A})^\times$, and $\#(\mathbf{A}/\wp\mathbf{A})^\times = q^{\deg(\wp)} - 1$, there exists an integer h with $0 \leq h \leq q^{\deg(\wp)} - 2$ such that

$$(13) \quad \mathcal{P}_\epsilon(0) \equiv \mathfrak{g}^h \pmod{\wp}.$$

Set

$$(14) \quad \epsilon = \left(\frac{C_{\mathfrak{g}}(\lambda_\wp)}{\lambda_\wp} \right)^{h-1} \alpha$$

for some $\alpha \in \mathbb{K}_\wp$. From Rosen [6, Proposition 12.6], we know that $\frac{C_{\mathfrak{g}}(\lambda_\wp)}{\lambda_\wp}$ is a unit in \mathcal{O}_\wp , and thus α is a unit in \mathcal{O}_\wp .

Let $\mathcal{P}_\alpha(x) \in \mathbf{A}[x]$ be the polynomial representing α , and set

$$(15) \quad \mathcal{Q}(x) = \left(\frac{C_{\mathfrak{g}}(x)}{x} \right)^{q^{\deg(\wp)+h-2}} \mathcal{P}_\alpha(x).$$

From Rosen [6, Proposition 12.11], one can write $C_{\mathfrak{g}}(x) \in \mathbf{A}[x]$ in the form

$$C_{\mathfrak{g}}(x) = \mathfrak{g}x + [\mathfrak{g}, 1]x^q + \dots + [\mathfrak{g}, \deg(\mathfrak{g}) - 1]x^{q^{\deg(\mathfrak{g})-1}} + [\mathfrak{g}, \deg(\mathfrak{g})]x^{q^{\deg(\mathfrak{g})}},$$

where $[\mathfrak{g}, i] \in \mathbf{A}$ for each $1 \leq i \leq \deg(\mathfrak{g})$. Thus

$$(16) \quad \frac{C_{\mathfrak{g}}(x)}{x} = \mathfrak{g} + [\mathfrak{g}, 1]x^{q-1} + \dots + [\mathfrak{g}, \deg(\mathfrak{g})]x^{q^{\deg(\mathfrak{g})}-1} \in \mathbf{A}[x].$$

Since $q^{\deg(\wp)} + h - 2 > 0$, we see that $\mathcal{Q}(x) \in \mathbf{A}[x]$.

We see from (14) that

$$\begin{aligned} \mathcal{Q}(\lambda_\wp) &= \left(\frac{C_{\mathfrak{g}}(\lambda_\wp)}{\lambda_\wp} \right)^{q^{\deg(\wp)+h-2}} \mathcal{P}_\alpha(\lambda_\wp) \\ &= \left(\frac{C_{\mathfrak{g}}(\lambda_\wp)}{\lambda_\wp} \right)^{q^{\deg(\wp)}-1} \epsilon, \end{aligned}$$

and thus

$$\mathcal{Q}(\lambda_\wp) - \left(\frac{C_{\mathfrak{g}}(\lambda_\wp)}{\lambda_\wp} \right)^{q^{\deg(\wp)}-1} \mathcal{P}_\epsilon(\lambda_\wp) = \mathcal{Q}(\lambda_\wp) - \left(\frac{C_{\mathfrak{g}}(\lambda_\wp)}{\lambda_\wp} \right)^{q^{\deg(\wp)}-1} \epsilon = 0.$$

Since $\mathcal{Q}(x) - \left(\frac{C_{\mathfrak{g}}(x)}{x} \right)^{q^{\deg(\wp)}-1} \mathcal{P}_\epsilon(x) \in \mathbf{A}[x]$, and the \wp -th cyclotomic polynomial $\Psi_\wp(x)$ is the minimal polynomial of λ_\wp , it follows from the above equation that $\Psi_\wp(x)$ divides $\mathcal{Q}(x) - \left(\frac{C_{\mathfrak{g}}(x)}{x} \right)^{q^{\deg(\wp)}-1} \mathcal{P}_\epsilon(x)$ in $\mathbf{A}[x]$. Thus there exists a polynomial, say $\mathcal{T}(x) \in \mathbf{A}[x]$ such that

$$(17) \quad \mathcal{Q}(x) - \left(\frac{C_{\mathfrak{g}}(x)}{x} \right)^{q^{\deg(\wp)}-1} \mathcal{P}_\epsilon(x) = \mathcal{T}(x)\Psi_\wp(x).$$

Setting $\mathcal{Z}(x) = \frac{C_{\mathfrak{g}}(x)}{x} \in \mathbf{A}[x]$, we see from (16) that

$$(18) \quad \mathcal{Z}(0) = \mathfrak{g}.$$

From Proposition 2.1, and (17), we deduce that

$$\mathcal{Q}(0) - \mathcal{Z}(0)^{q^{\deg(\wp)}-1} \mathcal{P}_\epsilon(0) = \mathcal{T}(0)\Psi_\wp(0) = \mathcal{T}(0)\wp \equiv 0 \pmod{\wp}.$$

From (13), (15), (18), and the above equation, we deduce that

$$\mathfrak{g}^{q^{\deg(\wp)+h-2}} \mathcal{P}_\alpha(0) = \mathcal{Z}(0)^{q^{\deg(\wp)+h-2}} \mathcal{P}_\alpha(0) = \mathcal{Q}(0) \equiv \mathcal{Z}(0)^{q^{\deg(\wp)}-1} \mathcal{P}_\epsilon(0) \equiv \mathfrak{g}^{q^{\deg(\wp)}+h-1} \pmod{\wp},$$

and thus

$$(19) \quad \mathcal{P}_\alpha(0) \equiv \mathfrak{g} \pmod{\wp}.$$

We know that $\sigma_{\mathfrak{g}}(\lambda_\wp) = C_{\mathfrak{g}}(\lambda_\wp)$, and thus $\frac{C_{\mathfrak{g}}(\lambda_\wp)}{\lambda_\wp} = \frac{\sigma_{\mathfrak{g}}(\lambda_\wp)}{\lambda_\wp}$. Since $\sigma_{\mathfrak{g}}$ is a generator of the Galois group $\text{Gal}(\mathbb{K}_\wp/\mathbf{k})$, it follows that

$$\text{Norm}_{\mathbb{K}_\wp/\mathbf{k}} \left(\frac{C_{\mathfrak{g}}(\lambda_\wp)}{\lambda_\wp} \right) = \text{Norm}_{\mathbb{K}_\wp/\mathbf{k}} \left(\frac{\sigma_{\mathfrak{g}}(\lambda_\wp)}{\lambda_\wp} \right) = 1.$$

Since ϵ is of norm 1, equation (14) and the above equation imply that α is also of norm 1. Applying Proposition 2.3, there exists an element $\delta \in \mathcal{O}_\varphi$ such that

$$(20) \quad \alpha = \frac{\delta}{\sigma_{\mathfrak{g}}(\delta)}.$$

Let $\mathcal{P}_\delta(x) \in \mathbf{A}[x]$ be the polynomial representing δ . Since $\delta = \mathcal{P}_\delta(\lambda_\varphi)$, one can write

$$(21) \quad \mathcal{P}_\delta(\lambda_\varphi) = \delta = \lambda_\varphi^e \eta,$$

where $\eta \in \mathcal{O}_\varphi$ such that $\gcd(\lambda_\varphi, \eta) = 1$, and e is a nonnegative integer.

Let $\mathcal{P}_\eta(x) \in \mathbf{A}[x]$ be the polynomial representing η . Since

$$\eta = \mathcal{P}_\eta(\lambda_\varphi) \equiv \mathcal{P}_\eta(0) \pmod{\lambda_\varphi},$$

and $\varphi \mathcal{O}_\varphi = (\lambda_\varphi \mathcal{O}_\varphi)^{q^{\deg(\varphi)} - 1}$, we see that if φ divides $\mathcal{P}_\eta(0)$, then the prime ideal $\lambda_\varphi \mathcal{O}_\varphi$ divides η , which is a contradiction. Hence

$$(22) \quad \gcd(\mathcal{P}_\eta(0), \varphi) = 1.$$

Note that the polynomial $\mathcal{P}_\eta(x)$ is not identical to zero since $\eta \neq 0$. Let $\mathfrak{c}(\mathcal{P}_\eta) \in \mathbf{A}$ be the content of the polynomial $\mathcal{P}_\eta(x)$, i.e., the greatest common divisor of all nonzero coefficients of $\mathcal{P}_\eta(x)$ in \mathbf{A} . Obviously $\mathfrak{c}(\mathcal{P}_\eta) \neq 0$. Set

$$(23) \quad \mathcal{R}(x) = \frac{\mathcal{P}_\eta(x)}{\mathfrak{c}(\mathcal{P}_\eta)} \in \mathbf{A}[x],$$

and let

$$(24) \quad \beta = \mathcal{R}(\lambda_\varphi) = \frac{\mathcal{P}_\eta(\lambda_\varphi)}{\mathfrak{c}(\mathcal{P}_\eta)} = \frac{\eta}{\mathfrak{c}(\mathcal{P}_\eta)} \in \mathcal{O}_\varphi = \mathbf{A}[\lambda_\varphi].$$

Let $\mathcal{P}_\beta(x) \in \mathbf{A}[x]$ be the polynomial representing β . Since $\deg(\mathcal{R}(x)) = \deg(\mathcal{P}_\eta(x)) \leq q^{\deg(\varphi)} - 2$, the uniqueness implies that $\mathcal{P}_\beta(x) = \mathcal{R}(x)$ (see Proposition 2.4). It follows from (23) that

$$(25) \quad \mathcal{P}_\beta(x) = \frac{\mathcal{P}_\eta(x)}{\mathfrak{c}(\mathcal{P}_\eta)}.$$

From (20) and (21), and since $\mathfrak{c}(\mathcal{P}_\eta) \in \mathbf{A}$, one sees that

$$\alpha = \frac{\lambda_\varphi^e \mathcal{P}_\eta(\lambda_\varphi)}{\sigma_{\mathfrak{g}}(\lambda_\varphi^e \mathcal{P}_\eta(\lambda_\varphi))} = \frac{\lambda_\varphi^e \mathcal{P}_\eta(\lambda_\varphi)}{\sigma_{\mathfrak{g}}(\lambda_\varphi^e) \sigma_{\mathfrak{g}}(\mathcal{P}_\eta(\lambda_\varphi))} = \left(\frac{\lambda_\varphi}{\sigma_{\mathfrak{g}}(\lambda_\varphi)} \right)^e \frac{\mathfrak{c}(\mathcal{P}_\eta) \mathcal{P}_\beta(\lambda_\varphi)}{\sigma_{\mathfrak{g}}(\mathfrak{c}(\mathcal{P}_\eta) \mathcal{P}_\beta(\lambda_\varphi))} = \left(\frac{\lambda_\varphi}{C_{\mathfrak{g}}(\lambda_\varphi)} \right)^e \frac{\mathcal{P}_\beta(\lambda_\varphi)}{\sigma_{\mathfrak{g}}(\mathcal{P}_\beta(\lambda_\varphi))},$$

and thus

$$\alpha = \left(\frac{\lambda_\varphi}{C_{\mathfrak{g}}(\lambda_\varphi)} \right)^e \frac{\mathcal{P}_\beta(\lambda_\varphi)}{\mathcal{P}_\beta(\sigma_{\mathfrak{g}}(\lambda_\varphi))} = \left(\frac{\lambda_\varphi}{C_{\mathfrak{g}}(\lambda_\varphi)} \right)^e \frac{\mathcal{P}_\beta(\lambda_\varphi)}{\mathcal{P}_\beta(C_{\mathfrak{g}}(\lambda_\varphi))}.$$

It therefore follows from (14) that

$$(26) \quad \epsilon = \left(\frac{\lambda_\varphi}{C_{\mathfrak{g}}(\lambda_\varphi)} \right)^{e-h+1} \frac{\mathcal{P}_\beta(\lambda_\varphi)}{\mathcal{P}_\beta(C_{\mathfrak{g}}(\lambda_\varphi))}.$$

By Rosen [6, Proposition 12.6], one knows that $\frac{\lambda_\varphi}{C_{\mathfrak{g}}(\lambda_\varphi)}$ is a unit in \mathcal{O}_φ , and thus

$$(i) \quad \frac{\mathcal{P}_\beta(\lambda_\varphi)}{\mathcal{P}_\beta(C_{\mathfrak{g}}(\lambda_\varphi))} \text{ is a unit in } \mathcal{O}_\varphi, \text{ or equivalently } \frac{\mathcal{P}_\beta(C_{\mathfrak{g}}(\lambda_\varphi))}{\mathcal{P}_\beta(\lambda_\varphi)} \text{ is a unit in } \mathcal{O}_\varphi.$$

From (22), (25), and since $\mathfrak{c}(\mathcal{P}_\eta)$ is the content of $\mathcal{P}_\eta(x)$, we deduce that

- (ii) $\gcd(\mathcal{P}_\beta(0), \varphi) = 1$.
- (iii) the content of the polynomial $\mathcal{P}_\beta(x)$ is 1.

Since $\mathcal{P}_\beta(x)$ satisfies all the conditions in Lemma 3.1, we deduce that $\beta = \mathcal{P}_\beta(\lambda_\wp)$ is a unit in \mathcal{O}_\wp , and thus $\frac{\mathcal{P}_\beta(\lambda_\wp)}{\mathcal{P}_\beta(C_{\mathfrak{g}}(\lambda_\wp))}$ belongs to the group \mathcal{G}_\wp . (Recall that \mathcal{G}_\wp is defined in Subsection 2.2.) By Corollary 3.5, there exist an integer ℓ with $0 \leq \ell \leq q^{\deg(\wp)} - 2$, and an element $\frac{\mathcal{P}(\lambda_\wp)}{\mathcal{P}(C_{\mathfrak{g}}(\lambda_\wp))} \in \mathcal{G}_\wp$ such that

$$\left(\frac{\lambda_\wp}{C_{\mathfrak{g}}(\lambda_\wp)} \right)^{e-h+1} = \left(\frac{\lambda_\wp}{C_{\mathfrak{g}}(\lambda_\wp)} \right)^\ell \frac{\mathcal{P}(\lambda_\wp)}{\mathcal{P}(C_{\mathfrak{g}}(\lambda_\wp))},$$

and it thus follows from (26) that

$$(27) \quad \epsilon = \left(\frac{\lambda_\wp}{C_{\mathfrak{g}}(\lambda_\wp)} \right)^\ell \left(\frac{\mathcal{P}(\lambda_\wp)}{\mathcal{P}(C_{\mathfrak{g}}(\lambda_\wp))} \frac{\mathcal{P}_\beta(\lambda_\wp)}{\mathcal{P}_\beta(C_{\mathfrak{g}}(\lambda_\wp))} \right).$$

Since \mathcal{G}_\wp is a multiplicative group, it follows from Proposition 2.5 and Proposition 2.7(iii) that there exists a polynomial $\mathcal{Q}(x) \in \mathbf{A}[x]$ of degree at most $q^{\deg(\wp)} - 2$ such that $\mathcal{Q}(\lambda_\wp)$ is a unit in \mathcal{O}_\wp , and

$$\frac{\mathcal{P}(\lambda_\wp)}{\mathcal{P}(C_{\mathfrak{g}}(\lambda_\wp))} \frac{\mathcal{P}_\beta(\lambda_\wp)}{\mathcal{P}_\beta(C_{\mathfrak{g}}(\lambda_\wp))} = \frac{\mathcal{Q}(\lambda_\wp)}{\mathcal{Q}(C_{\mathfrak{g}}(\lambda_\wp))}.$$

Hence we deduce from (27) that

$$\epsilon = \left(\frac{\lambda_\wp}{C_{\mathfrak{g}}(\lambda_\wp)} \right)^\ell \left(\frac{\mathcal{Q}(\lambda_\wp)}{\mathcal{Q}(C_{\mathfrak{g}}(\lambda_\wp))} \right),$$

which proves the first part of the theorem.

We now prove the uniqueness. Assume that there exist another integer ℓ_\star with $0 \leq \ell_\star \leq q^{\deg(\wp)} - 2$, and another polynomial $\mathcal{Q}_\star(x) \in \mathbf{A}[x]$ of degree at most $q^{\deg(\wp)} - 2$ with $\mathcal{Q}_\star(\lambda_\wp)$ being a unit in \mathcal{O}_\wp such that

$$(28) \quad \epsilon = \left(\frac{\lambda_\wp}{C_{\mathfrak{g}}(\lambda_\wp)} \right)^\ell \left(\frac{\mathcal{Q}(\lambda_\wp)}{\mathcal{Q}(C_{\mathfrak{g}}(\lambda_\wp))} \right) = \left(\frac{\lambda_\wp}{C_{\mathfrak{g}}(\lambda_\wp)} \right)^{\ell_\star} \left(\frac{\mathcal{Q}_\star(\lambda_\wp)}{\mathcal{Q}_\star(C_{\mathfrak{g}}(\lambda_\wp))} \right).$$

Hence

$$(29) \quad \left(\frac{C_{\mathfrak{g}}(\lambda_\wp)}{\lambda_\wp} \right)^\ell \left(\frac{\mathcal{Q}(C_{\mathfrak{g}}(\lambda_\wp))}{\mathcal{Q}(\lambda_\wp)} \right) = \left(\frac{C_{\mathfrak{g}}(\lambda_\wp)}{\lambda_\wp} \right)^{\ell_\star} \left(\frac{\mathcal{Q}_\star(C_{\mathfrak{g}}(\lambda_\wp))}{\mathcal{Q}_\star(\lambda_\wp)} \right).$$

By Rosen [6, Proposition 12.11], $C_{\mathfrak{g}}(x) \in \mathbf{A}[x]$ can be written in the form

$$C_{\mathfrak{g}}(x) = \mathfrak{g}x + [\mathfrak{g}, 1]x^q + \dots + [\mathfrak{g}, \deg(\mathfrak{g})]x^{q^{\deg(\mathfrak{g})}},$$

where the $[\mathfrak{g}, i]$ are in \mathbf{A} , and $[\mathfrak{g}, \deg(\mathfrak{g})] \in \mathbb{F}_q^\times$ is the leading coefficient of \mathfrak{g} . It follows that

$$(30) \quad C_{\mathfrak{g}}(0) = 0,$$

and

$$(31) \quad \frac{C_{\mathfrak{g}}(\lambda_\wp)}{\lambda_\wp} \equiv \mathfrak{g} \pmod{\lambda_\wp}.$$

Furthermore we deduce from Lemma 3.6 that $\gcd(\mathcal{Q}(0), \wp) = 1$ and $\gcd(\mathcal{Q}_\star(0), \wp) = 1$. In particular this implies that $\mathcal{Q}(0), \mathcal{Q}_\star(0)$ are nonzero elements in \mathbf{A} . Hence it follows from (29), (30), and (31) that

$$\mathfrak{g}^\ell \equiv \mathfrak{g}^{\ell_\star} \pmod{\lambda_\wp}.$$

Since $\wp \mathcal{O}_\wp = (\lambda_\wp \mathcal{O}_\wp)^{q^{\deg(\wp)}-1}$ (see Rosen [6, Proposition 12.7]), we deduce that

$$\mathfrak{g}^\ell \equiv \mathfrak{g}^{\ell_\star} \pmod{\wp}.$$

Without loss of generality, we assume that $\ell \geq \ell_\star$. If $\ell > \ell_\star$, then

$$\mathfrak{g}^{\ell-\ell_\star} \equiv 1 \pmod{\wp},$$

and since \mathfrak{g} is a primitive root modulo \wp , the above equation implies that $\#(\mathbf{A}/\wp \mathbf{A})^\times = q^{\deg(\wp)} - 1$ divides $\ell - \ell_\star$. This is a contradiction since $0 < \ell - \ell_\star < q^{\deg(\wp)} - 1$. Hence

$$(32) \quad \ell = \ell_\star.$$

By (28), and since $\sigma_{\mathfrak{g}}(\lambda_\wp) = C_{\mathfrak{g}}(\lambda_\wp)$, we deduce that

$$\frac{\mathcal{Q}(\lambda_\wp)}{\mathcal{Q}_\star(\lambda_\wp)} = \frac{\mathcal{Q}(C_{\mathfrak{g}}(\lambda_\wp))}{\mathcal{Q}_\star(C_{\mathfrak{g}}(\lambda_\wp))} = \sigma_{\mathfrak{g}} \left(\frac{\mathcal{Q}(\lambda_\wp)}{\mathcal{Q}_\star(\lambda_\wp)} \right).$$

Thus the unit $\frac{\mathcal{Q}(\lambda_\wp)}{\mathcal{Q}_\star(\lambda_\wp)}$ in \mathcal{O}_\wp is invariant under the action of $\sigma_{\mathfrak{g}}$. Since $\sigma_{\mathfrak{g}}$ is a generator of the cyclic group $\text{Gal}(\mathbb{K}_\wp/\mathbf{k})$, the unit $\frac{\mathcal{Q}(\lambda_\wp)}{\mathcal{Q}_\star(\lambda_\wp)}$ is also invariant under the action of each member of $\text{Gal}(\mathbb{K}_\wp/\mathbf{k})$, and thus $\frac{\mathcal{Q}(\lambda_\wp)}{\mathcal{Q}_\star(\lambda_\wp)}$ is a unit in \mathbf{A} . This implies that $\frac{\mathcal{Q}(\lambda_\wp)}{\mathcal{Q}_\star(\lambda_\wp)} \in \mathbb{F}_q^\times$, and therefore there exists a unit $v \in \mathbb{F}_q^\times$ such that

$$(33) \quad \mathcal{Q}_\star(\lambda_\wp) = v \mathcal{Q}(\lambda_\wp).$$

Set $\kappa = \mathcal{Q}_\star(\lambda_\wp)$. By the assumption, we know that κ is a unit in \mathcal{O}_\wp . Since the polynomial $\mathcal{Q}_\star(x)$ is of degree at most $q^{\deg(\wp)} - 2$, it follows from Proposition 2.4 that $\mathcal{Q}_\star(x) = \mathcal{P}_\kappa(x)$, where $\mathcal{P}_\kappa(x) \in \mathbf{A}[x]$ is the polynomial representing κ .

On the other hand, we know from (33) that $\kappa = v \mathcal{Q}(\lambda_\wp)$. Note that $v \mathcal{Q}(x)$ is a polynomial in $\mathbf{A}[x]$ of degree at most $q^{\deg(\wp)} - 2$ since $v \in \mathbb{F}_q^\times$. Hence repeating the same arguments as above, one sees that $v \mathcal{Q}(x) = \mathcal{P}_\kappa(x)$, and thus

$$(34) \quad \mathcal{Q}_\star(x) = v \mathcal{Q}(x).$$

The second part of the theorem follows immediately from (32) and (34). \square

Recall that the multiplicative group \mathcal{G}_\wp consists of all elements $\frac{\mathcal{Q}(\lambda_\wp)}{\mathcal{Q}(C_{\mathfrak{g}}(\lambda_\wp))}$, where $\mathcal{Q}(x)$ is a polynomial in $\mathbf{A}[x]$ such that $\mathcal{Q}(\lambda_\wp)$ is a unit in \mathcal{O}_\wp . The next result follows immediately from Theorem 3.7.

Corollary 3.8. *Let ϵ be a unit in \mathcal{O}_\wp of norm 1. Then there exist an integer ℓ with $0 \leq \ell \leq q^{\deg(\wp)} - 2$, and an element $\kappa \in \mathcal{G}_\wp$ such that the following are true:*

(i) ϵ can be represented in the form

$$\epsilon = \left(\frac{\lambda_\wp}{C_{\mathfrak{g}}(\lambda_\wp)} \right)^\ell \kappa.$$

(ii) The representation of ϵ in (i) is unique; more precisely, if there exist another integer ℓ_\star with $0 \leq \ell_\star \leq q^{\deg(\wp)} - 2$, and another element $\kappa_\star \in \mathcal{G}_\wp$ such that

$$\epsilon = \left(\frac{\lambda_\wp}{C_{\mathfrak{g}}(\lambda_\wp)} \right)^{\ell_\star} \kappa_\star,$$

then $\ell_\star = \ell$ and $\kappa_\star = \kappa$.

Corollary 3.8 can be interpreted in terms of group theory.

Corollary 3.9.

- (i) \mathcal{G}_\wp is a subgroup of $\mathcal{U}_\star(\mathcal{O}_\wp)$ such that $[\mathcal{U}_\star(\mathcal{O}_\wp) : \mathcal{G}_\wp] = q^{\deg(\wp)} - 1$. (Recall that $\mathcal{U}_\star(\mathcal{O}_\wp)$ is the group of units of norm 1 in \mathcal{O}_\wp .)
- (ii) The quotient group $\mathcal{U}_\star(\mathcal{O}_\wp)/\mathcal{G}_\wp$ is cyclic of order $q^{\deg(\wp)} - 1$; furthermore $\mathcal{U}_\star(\mathcal{O}_\wp)/\mathcal{G}_\wp$ is generated by $\frac{\lambda_\wp}{C_\mathfrak{g}(\lambda_\wp)}\mathcal{G}_\wp$.

Hilbert's Satz 90 (see Lang [4]) tells us that for a unit $\epsilon \in \mathcal{U}_\star(\mathcal{O}_\wp)$, there exists an element $\delta \in \mathcal{O}_\wp$ such that $\epsilon = \frac{\delta}{\sigma_\mathfrak{g}(\delta)}$ (see Proposition 2.3). The next result is a refinement of Hilbert's Satz 90 for the extension $\mathbb{K}_\wp/\mathbf{k}$, which gives a sufficient and necessary condition under which an element in \mathcal{O}_\wp is a quotient of conjugate units.

Corollary 3.10. *Let $\epsilon \in \mathcal{U}_\star(\mathcal{O}_\wp)$. Then ϵ is the quotient of conjugate units in \mathcal{O}_\wp if and only if $\mathcal{P}_\epsilon(0) \equiv 1 \pmod{\wp}$, where $\mathcal{P}_\epsilon(x) \in \mathbf{A}[x]$ is the polynomial representing ϵ .*

Proof. Assume that ϵ is the quotient of conjugate units in \mathcal{O}_\wp , i.e., $\epsilon = \frac{\delta}{\sigma_{\mathfrak{g}^e}(\delta)}$ for some unit $\delta \in \mathcal{O}_\wp$, and some integer e with $0 \leq e \leq q^{\deg(\wp)} - 2$. (Recall that $\sigma_\mathfrak{g}$ is a generator of the Galois group $\text{Gal}(\mathbb{K}_\wp/\mathbf{k})$.) If $e = 0$, then $\epsilon = 1$, and it is easy to see that the polynomial $\mathcal{P}_\epsilon(x) = \mathcal{P}_1(x) = 1$. Hence $\mathcal{P}_1(0) \equiv 1 \pmod{\wp}$.

We now consider the case where $e \geq 1$. Set

$$\alpha = \prod_{i=0}^{e-1} \sigma_{\mathfrak{g}^i}(\delta) = \delta \cdot \sigma_\mathfrak{g}(\delta) \cdots \sigma_{\mathfrak{g}^{e-1}}(\delta).$$

One can immediately verify that α is a unit in \mathcal{O}_\wp , and

$$(35) \quad \epsilon = \frac{\delta}{\sigma_{\mathfrak{g}^e}(\delta)} = \frac{\alpha}{\sigma_\mathfrak{g}(\alpha)}.$$

By Proposition 2.7, $\frac{\alpha}{\sigma_\mathfrak{g}(\alpha)}$ belongs to the group \mathcal{G}_\wp . Since $\epsilon = \mathcal{P}_\epsilon(\lambda_\wp)$, we deduce from (35) that

$$(36) \quad \mathcal{P}_\epsilon(\lambda_\wp) = \frac{\alpha}{\sigma_\mathfrak{g}(\alpha)} = \frac{\mathcal{P}_\alpha(\lambda_\wp)}{\mathcal{P}_\alpha(C_\mathfrak{g}(\lambda_\wp))},$$

where $\mathcal{P}_\alpha(x)$ is the polynomial representing α . Following the same arguments as in the proof of Theorem 3.7 (see equation (30)), we deduce that $C_\mathfrak{g}(0) = 0$. Using Lemma 3.6, we know that $\gcd(\mathcal{P}_\alpha(0), \wp) = 1$; hence $\gcd(\mathcal{P}_\alpha(0), \lambda_\wp) = 1$ since $\wp\mathcal{O}_\wp = (\lambda_\wp\mathcal{O}_\wp)^{q^{\deg(\wp)}-1}$ and $\lambda_\wp\mathcal{O}_\wp$ is a prime ideal in \mathcal{O}_\wp (see Rosen [6, Proposition 12.7]). In particular, this implies that $\mathcal{P}_\alpha(0) \not\equiv 0 \pmod{\lambda_\wp}$. By (36), we see that

$$\mathcal{P}_\epsilon(0) \equiv \mathcal{P}_\epsilon(\lambda_\wp) = \frac{\mathcal{P}_\alpha(\lambda_\wp)}{\mathcal{P}_\alpha(C_\mathfrak{g}(\lambda_\wp))} \equiv \frac{\mathcal{P}_\alpha(0)}{\mathcal{P}_\alpha(C_\mathfrak{g}(0))} = \frac{\mathcal{P}_\alpha(0)}{\mathcal{P}_\alpha(0)} = 1 \pmod{\lambda_\wp},$$

and thus

$$\mathcal{P}_\epsilon(0) \equiv 1 \pmod{\wp}.$$

Conversely assume that $\epsilon \in \mathcal{U}_\star(\mathcal{O}_\wp)$ such that

$$(37) \quad \mathcal{P}_\epsilon(0) \equiv 1 \pmod{\wp}.$$

By Theorem 3.7, one can write ϵ in the form

$$(38) \quad \epsilon = \mathcal{P}_\epsilon(\lambda_\wp) = \left(\frac{\lambda_\wp}{C_{\mathfrak{g}}(\lambda_\wp)} \right)^\ell \frac{\mathcal{Q}(\lambda_\wp)}{\mathcal{Q}(C_{\mathfrak{g}}(\lambda_\wp))},$$

where ℓ is an integer such that $0 \leq \ell \leq q^{\deg(\wp)} - 2$, and $\mathcal{Q}(x)$ is a polynomial in $\mathbf{A}[x]$ of degree at most $q^{\deg(\wp)} - 2$ such that $\mathcal{Q}(\lambda_\wp)$ is a unit in \mathcal{O}_\wp . One can write (38) in the form

$$(39) \quad \left(\frac{C_{\mathfrak{g}}(\lambda_\wp)}{\lambda_\wp} \right)^\ell \mathcal{P}_\epsilon(\lambda_\wp) = \frac{\mathcal{Q}(\lambda_\wp)}{\mathcal{Q}(C_{\mathfrak{g}}(\lambda_\wp))}.$$

Following the same arguments as in the proof of Theorem 3.7 (see equation (31)), we know that

$$\frac{C_{\mathfrak{g}}(\lambda_\wp)}{\lambda_\wp} \equiv \mathfrak{g} \pmod{\lambda_\wp},$$

and thus

$$(40) \quad \left(\frac{C_{\mathfrak{g}}(\lambda_\wp)}{\lambda_\wp} \right)^\ell \equiv \mathfrak{g}^\ell \pmod{\lambda_\wp}.$$

Repeating the same arguments as in the first part of this proof, one can show that

$$\frac{\mathcal{Q}(\lambda_\wp)}{\mathcal{Q}(C_{\mathfrak{g}}(\lambda_\wp))} \equiv \frac{\mathcal{Q}(0)}{\mathcal{Q}(C_{\mathfrak{g}}(0))} = \frac{\mathcal{Q}(0)}{\mathcal{Q}(0)} = 1 \pmod{\lambda_\wp},$$

and it thus follows from (39) and (40) that

$$(41) \quad \mathfrak{g}^\ell \mathcal{P}_\epsilon(0) \equiv 1 \pmod{\lambda_\wp}.$$

Since $\mathfrak{g}^\ell \mathcal{P}_\epsilon(0) \in \mathbf{A}$, and $\wp \mathcal{O}_\wp = (\lambda_\wp \mathcal{O}_\wp)^{q^{\deg(\wp)} - 1}$ (see Rosen [6, Proposition 12.7]), we deduce from (41) that

$$\mathfrak{g}^\ell \mathcal{P}_\epsilon(0) \equiv 1 \pmod{\wp},$$

and it thus follows from (37) that

$$\mathfrak{g}^\ell \equiv 1 \pmod{\wp}.$$

Since \mathfrak{g} is a generator of the cyclic group $(\mathbf{A}/\wp \mathbf{A})^\times$, and the order of $(\mathbf{A}/\wp \mathbf{A})^\times$ is $q^{\deg(\wp)} - 1$, the above equation implies that $\ell = 0$. Therefore we deduce from (38) that

$$\epsilon = \frac{\mathcal{Q}(\lambda_\wp)}{\mathcal{Q}(C_{\mathfrak{g}}(\lambda_\wp))} = \frac{\mathcal{Q}(\lambda_\wp)}{\mathcal{Q}(\sigma_{\mathfrak{g}}(\lambda_\wp))} = \frac{\mathcal{Q}(\lambda_\wp)}{\sigma_{\mathfrak{g}}(\mathcal{Q}(\lambda_\wp))} = \frac{\kappa}{\sigma_{\mathfrak{g}}(\kappa)},$$

where $\kappa = \mathcal{Q}(\lambda_\wp)$ is a unit in \mathcal{O}_\wp . Thus our contention follows. \square

Remark 3.11. Corollary 3.10 is a function field analogue of Newman [5, Corollary, p.357].

REFERENCES

- [1] D.M. GOLDSCHMIDT, *Algebraic functions and projective curves*, Graduate Texts in Mathematics, **215**, Springer-Verlag, New York, (2003).
- [2] D. GOSS, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], **35**, Springer-Verlag, Berlin, (1996).
- [3] D.R. HAYES, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. **189** (1974), 77–91.
- [4] S. LANG, *Algebra*, Addison-Wesley Publishing Co., Inc., Reading, Mass. (1965).
- [5] M. NEWMAN, *Cyclotomic units and Hilbert's Satz 90*, Acta Arith. **41** (1982), no. 4, 353–357.
- [6] M. ROSEN, *Number theory in function fields*, Graduate Texts in Mathematics, **210**, Springer-Verlag, New York (2002).
- [7] D.S. THAKUR, *Function Field Arithmetic*, World Scientific Publishing Co., Inc., River Edge, NJ, (2004).

DEPARTMENT OF MATHEMATICS, THE UNIVERSITY OF TEXAS AT AUSTIN, AUSTIN, TX 78712, USA
E-mail address: dongquan.ngoc.nguyen@gmail.com